Release A CDR RID Report

Date Last Modified 11/30/95
Originator Henley, Gordon
Phone No 301-982-5414 ext 259
Organization IV&V/Intermetrics
E Mail Address gdh@cclink.gblt.inmet.com
Document Security Architecture

RID ID **CDR** 89
Review SDPS/CSMS
Originator Ref IVVRID-GH-1
Priority 2

Section NA **Page** NA **Figure Table** NA

Category Name ECS System-Level **Actionee** ECS
Sub Category
Subject Security Architecture

Description of Problem or Suggestion:

Security is not integrated throughout the design in the 305 document. In the CDR presentation, HAIS referenced the Security Plan as the source of system wide security information. However, while the plan presents the ECS DCE concept and the Kerberos product, but it does not explain how all the security features of the developed and COTs products (e.g.. various vendor UNIX type operating systems, Sybase DBMS) fit together. The Security Plan does not explain how ECS program security will fit with NASA security procedures and provisions and does not plan for implementing integrated security for the end-users.

There is no system-wide perspective or view addressing how the ECS software design complies with system security requirements. Currently, the indirect method to obtain an assessment is by performing an analysis of the Level 3 to Level 4 requirement traceability (in CDR RTM baseline) as well as an analysis of the traceability from Level 4 requirements to design components. Since this traceability can span a number of components, an overall assessment can only be performed once all components have been analyzed. Still, there is no clear and comprehensive documentation of how security requirements are implemented in the design. Issues relating to COTS integration with the security architecture were mentioned, but not in detail. There is no discussion of security certification or specialized test approach for Release A security features.

Originator's Recommendation

Document and provide traceability information in conjunction with design concepts and rationale, possibly in the security plan or in the overview design documentation. Provide detail on issues, problems, and plans for used COTS and COTS-compatability in the security architecture. Develop a top-level test concept for security certification tests.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Jacob Eisenstein **HAIS Schedule** 9/27/95
HAIS R. E. Richard Meyer **HAIS Response Date** 11/21/95

1. Requirements traces are provided in DID 305, as requested by the Government (see Contract Data Requirements List). The Release A Security Plan (215-CD-001-001) provides a mapping from Level 3 to Level 4 requirements, as of June 1995. The traces will be updated by the Release B design documents and the Release B Security Plan.

2. An overview of the technical approach to system security, including an overview of the security architecture are provided in the Security Plan, as well as the Overview of Release A SDPS and CSMS System Design Specification for the ECS Project (305-CD-004-001), Sections 6.2 and 6.3 (July 1995). This Overview maps threats to countermeasures and assigns implementation responsibility to specific Release A CSCI. DCE provides the basis for all internal ECS security, and Section 6.2. in the Overview explains at a high level how it will be employed. In particular, DCE provides security across the operating systems employed by ECS, except as noted in Section 6.2.5 of the Overview. Also, ECS will interface with external entities which do not employ comparable security mechanisms. The general gateway architecture for handling security policies for external interfaces is described in Section 6.3 of the Overview. At the time of CDR, TSDIS / ECS interface security issues were still; pending; a detail design of the security gateway, therefore, was not presented. In the meantime, the issues have been resolved and will be documented in the Post CDR update of the TSDIS ICD. The security gateway design is now scheduled for Phase 3 of the Release A implementation which starts in March 1, 1996. The CSS subdocument of DID 305 (305-CD-012-001) will be updated to reflect that design.

It should also be noted that in the context of the ECS architectures, users will have no direct access to the Sybase DBMS - all accesses will be performed via the data server, advertising server, etc. These components will implement any additional access controls that may be required beyond DCE (e.g., where security provisions are needed at the data level). The relevant design objects are defined in the CSS design document Section 4.2.2 (305-CD-012-001).

ECS will take advantage of the various capabilities offered by Unix and its utilities in enforcing security at the ECS platform login level (e.g., login scripts, file protection, etc.). Host security will also be assured, for example, by disabling ports not authorized for access to that host, through appropriate configuration of the host operating system. These aspects, as well as the specific groups and ACLs that will be established are considered part of the implementation, not the design

3. The design will be tested against the security requirements at the requirements Level 3 and Level 4. The test approaches are described in the respective security plans (DID 319, DID 402). The Security Plan describes how they fit into the Security System Acceptance. No requirements for the security certification process beyond what is described in the Security Plan have been levied on the ECS Release A at this time.

Status **Closed** **Date Closed** **11/30/95** **Sponsor** **Schroeder**

****** **Attachment if any** ******